SID POLICY & STANDARDS FOR RISK MANAGEMENT

For The

State Of California

Health and Human Services Data Center (HHSDC)

Systems Integration Division (SID)

July 16, 2003

Prepared for:
The Management Steering Council (MSC)
Health & Human Services Data Center
Systems Integration Division
1651 Alhambra Blvd
Sacramento, California 95816

Prepared by:
The Best Practices Support Group (BPSG)
The Quality Assurance Working Group (QAWG)

APPROVAL

Steve C Howe 8-13-03

Steve Howe, Executive Sponsor Date

Loney 7/16/03

Carol Loney, CMIPS Project Date

for Kathy Curtis 7/16/03

Bob Ferguson, CWS/CMS Project Date

Kathy Curtis 7/16/03

Kathy Curtis, CWS/CMS M&O Project Date

Trisha Edgerton 9/15/03

Trisha Edgerton, CWS/CMS Procurement Project Date

Chris Dunham 7/16/03

Chris Dunham, EBT Project Date

Parr 7/16/2003

Linda Parr, ISAWS Project Date

Kathy Saito, POST Project Date

Cris Jensen 7-16-2003

Cris Jensen, SAWS Project Date

George Christie

George Christie, SFIS Project Date

Richard A Ke 7-16-2003

Richard Keene, WDTIP Project Date

REVISION HISTORY

Rev. #	Description of Change	Date
1.0	Baseline	July 16, 2003

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Adoption of SID Policy

As part of their ongoing commitment to process improvement and quality within the division, the Systems Integration Division (SID) is adopting this SID Policy & Standards for Risk Management. This policy will help to clarify and enhance our current practices, and continue to align our organization with the Software Engineering Institute's Capability Maturity Model (SEI's CMM), and ensure compliance with the Department of Finance (DOF) Information Technology Project Oversight Framework, Budget Letter 03-04, dated Feb 7, 2003.

1.2 Applicability

This policy applies to all SID projects effective the date of this policy. Projects that are in the middle of an [1]SID life cycle process (at the effective date of this policy) are required to demonstrate due diligence in complying with this policy within 30 days, to the degree that it does not jeopardize their ability to satisfy prior project commitments. The SID Assistant Director will consider special situations for non-compliance on a case-by-case basis.

Projects that are in the Maintenance & Operations (M&O) life cycle phase must, as a minimum, assess compliance with this policy on an annual basis. All other projects must, as a minimum, assess compliance with this policy at the start of a new life cycle phase.

1.3 Policy Statement

The Systems Integration Division (SID) has created this policy to be in compliance with the SEI CMM methodology, as well as, the Department Of Finance (DOF) Information Technology Project Oversight Framework (Budget Letter 03-04, dated Feb 7, 2003). SID projects will adopt (and tailor as needed) the Software Engineering Institute's (SEI's) Risk Management Paradigm as the preferred source of guidance for successfully implementing risk management.

Projects in SID must demonstrate compliance to the SID Policy & Standards for Risk Management and SID CMM policies outlined on the Best Practices web site (http://bpweb/SID_Policy_Stds.htm and http://www.bestpractices.cahwnet.gov/SID_Policy_Stds.htm) and document their risk management strategies in a formal project Risk Management Plan.

The Project Director/Manager will appoint responsibility for risk management to an individual, with a named position with roles & responsibilities identified in the Project Plan and the project Risk Management Plan.

[1] The SID Best Practices Website defines the typical lifecycle for software acquisition projects in the organization. Explanation of each of the lifecycle phases can be found @ http://www.bestpractices.cahwnet.gov/processes.htm.

1.4 Reference Documents

- Department of Finance (DOF) Information Technology Project Oversight Framework, Budget Letter 03-04, dated Feb 7, 2003, DOF.
- Software Acquisition - Capability Maturity Model (SA-CMM), Key Process Area 3.4 - Acquisition Risk Mgmt, April 1999, SEI.
- Taxonomy-Based Risk Identification, June 1993, SEI.
- Project Management Body Of Knowledge (PMBOK), Project Risk Management, 2000, Project Management Institute (PMI).
- Software Risk Evaluation (SRE) Method Description, December 1999, SEI.
- Continuous Risk Management Guidebook (Dorofee, 1996).
- SID CMM policies, Best Practices web site (http://bpweb and http://www.bestpractices.cahwnet.gov), SID.
- SID Standards for Risk Management, Best Practices web site (http://bpweb and http://www.bestpractices.cahwnet.gov) , SID.

2 RISK MANAGEMENT PROCESS

Projects will adopt the following SEI Risk Paradigm that includes six process areas for risk management as defined below:

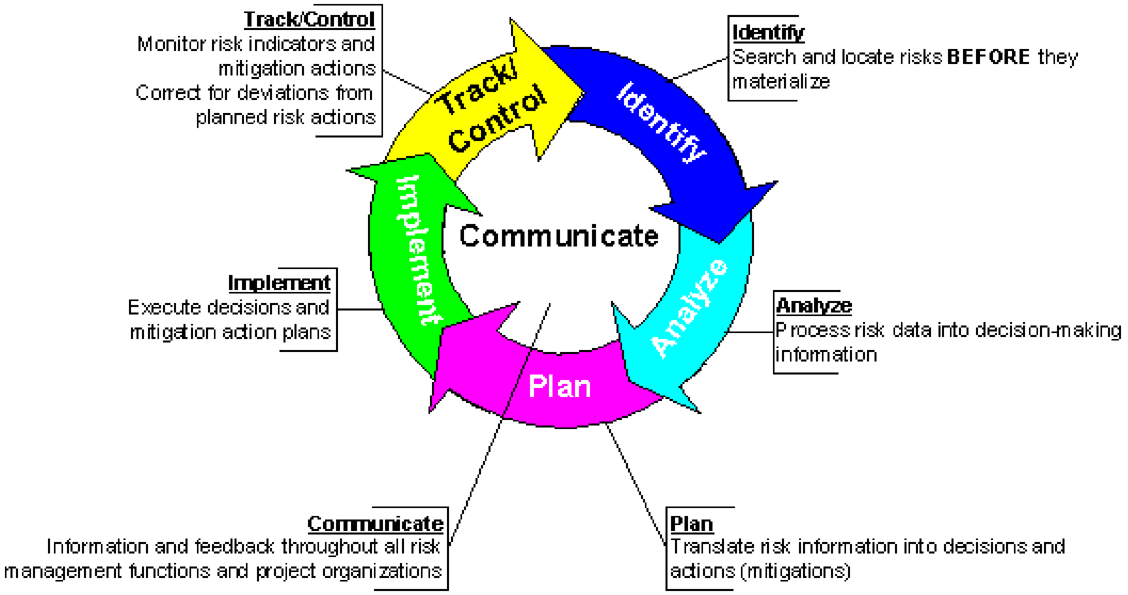

Track/Control
Monitor risk indicators and mitigation actions
Correct for deviations from planned risk actions
Identify
Search and locate risks BEFORE they materialize
Implement
Execute decisions and mitigation action plans
Analyze
Process risk data into decision-making information
Communicate
Information and feedback throughout all risk management functions and project organizations
Plan
Translate risk information into decisions and actions (mitigations)
Track/ Control
Identify
Analyze
Plan
Implement
Communicate

Figure 1

3 IDENTIFY RISKS

Projects will identify potential project risks before they become problems. Risk identification will involve a process where issues and concerns about a project are transformed into a list of tangible risks.

3.1 Risk Management Tools

Projects will record their project risk management activities for each of the process areas in a Project Risk Database (PRD).

Projects shall participate in the SID Project Office Support Tool (POST) initiative to the maximum extent possible in an effort to transition all projects to a common tool for managing risks. Until this initiative is completed, projects may use other tools that meet project needs.

3.2 SEI Risk Taxonomy

Projects will use the SEI's Taxonomy-Based Risk Identification schema (with associated questions) as a best practices tool for identifying potential project risks. The primary use of the SEI Taxonomy will be to aid projects in the identification of potential risks, NOT in mandating categories for managing risks. The outline of the Taxonomy-Based Risk Identification schema is shown in Appendix A of this document. Helpful hints when using the taxonomy exercise are noted below.

- Be careful to tailor the questions for each peer group before answering all the questions. Projects are to maintain their own tailored list of questions.
- Conduct interviews by peer groups (e.g., management, implementation team, technical staff, and administration staff).
- Aggregate results from each of the peer groups and build a single list of risks for the entire project (this eliminates the identification of risk items being attributable to a single person, and allows for elimination of overlapping or conflicting risks).

3.3 Project-Unique Identification of Risks

Projects are strongly encouraged to use other tools (e.g., brainstorming) for identifying risks as a way to identify risk areas not specifically addressed by the Risk Taxonomy. Risk areas unique to SID include such things as:

- Business Process Re-engineering (BPR)
- Implementation
- Project-specific functional areas
- Advocate groups

4 ANALYZE RISKS

Step 2 is for projects to analyze and transform risk items (identified in figure 1) into information that can be used to aid decision-making and to validate the risk information. Projects will incorporate the guidance provided below into their project Risk Management Plan. Recommendations for mitigating and measuring risk items, and reviewing risk item information will also be required in this step.

4.1 Risk Classification

Projects shall classify risks using the following categories taken from the DOF IT Project Oversight Framework, Appendix C (*Categories and Examples of Risk*) and *Appendix D (Project Risk List)*. However, projects may also add additional classifications to meet the unique needs of the project. Projects shall consult their oversight representative(s) before finalizing risk categories.

- Plan/Schedule
- Organization and Management
- Development Environment
- User Involvement
- Contractor Performance
- Requirements Management
- Product Characteristics
- External Environment
- Personnel
- Design and Implementation
- Process

4.2 Risk Impact

Projects will adopt the following rating when assigning impacts to identified risks.

High- The risk represents a significant negative impact on project budget, schedule, or quality.

Medium- The risk's material impacts would significantly affect users, clients, or other key stakeholders.

Low- The risk does not represent a significant or material impact on project budget, schedule or quality.

4.3 Probability

Projects will adopt the following rating when assigning probability to identified risks.

High- The risks are almost certain or very likely to occur.

Medium- The risks may occur or have a 50/50 chance of occurring.

Low- The risks are unlikely to occur or will probably not occur.

4.4 Timeframe

Projects will define the timeframes when risks could materialize and a mitigation/contingency plan must be implemented according to the following ratings

Short-Term – The risk is most likely to occur in less than 6 months.

Medium-Term –The risk is most likely to materialize between 6 months to 1 year from now.

Long-Term –The risk is most likely to materialize in a period of greater than 1 year.

4.5 Risk Exposure

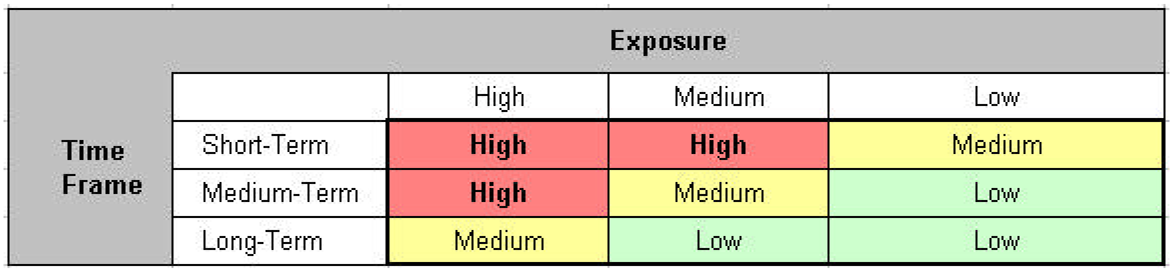
Projects will create a risk exposure matrix from the risk attributes of impact and probability. Projects will assign the following risk exposure ratings as shown in the matrix below. Projects not tracking timeframes will use this chart to establish risk priority.

		Probability		
		High	Medium	Low
Impact	High	**High**	**High**	Medium
	Medium	**High**	Medium	Low
	Low	Medium	Low	Low

Reference: Department Of Finance, Information Technology Project Oversight Framework, Section 5 - Risk Mgmt and Escalation Procedures.

4.6 Risk Severity (Priority)

Projects will define risk severity as a function of Risk Exposure and Timeframe for determining the relative PRIORITY of the identified risks. Projects will create and assign the following risk severity ratings as shown in the matrix below.



		Exposure		
		High	Medium	Low
Time Frame	Short-Term	**High**	**High**	Medium
	Medium-Term	**High**	Medium	Low
	Long-Term	Medium	Low	Low

5 Risk Management Planning For Mitigation/Contingencies

Projects will document their risk mitigation/contingency strategy as directed by this policy in the project's Risk Management Plan. Projects will make provisions for the mitigation and ownership of risks. Projects will ensure as a minimum the following mitigation/contingency planning is performed and documented:

- Assignment of ownership to risks,
- Process for development of risk mitigation/contingency strategies and measurements (Note: Acceptable actions include: taking action to avoid the risk altogether, accepting the risk without action, watching for a period of time before deciding what to do if anything, or actively mitigating the impacts of a risk),
- Process for review and approval of risk mitigations/contingencies and measurements,
- Process for translating of mitigations/contingencies into documented action plans, and
- Process for recording risk information changes in a Project Risk Database (PRD).

6 Implementing Risk Management

Projects will implement their risk plans to actively mitigate risks as they become realized. Projects will execute their risk mitigation/contingency action plans and record risk information changes in a Project Risk Database (PRD).

7 Tracking & Controlling Risks

Projects will track and control the risk management process to insure that all steps are being followed and, as a result, risks are being mitigated. As a minimum, projects will oversee and track:

- Action plan execution,
- Re-assessment of risks,
- Reporting of risk status, and
- Recording of risk information changes in a Project Risk Database (PRD).

7.1 Risks and the Management Steering Council (MSC)

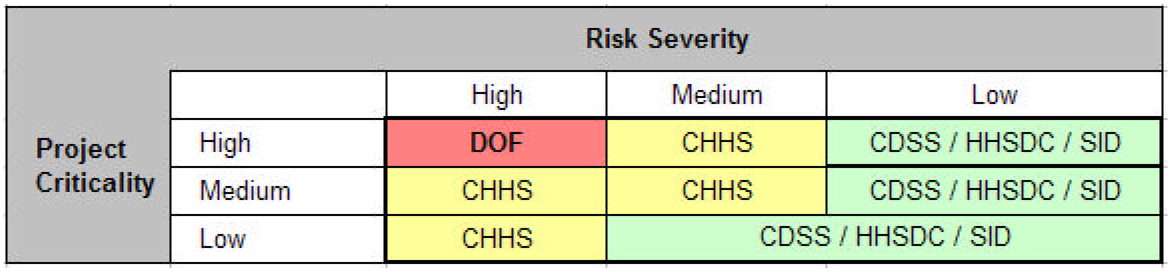
The Management Steering Council (MSC) will track risks that impact multiple projects in the SID organization. Risk affecting multiple SID projects will be periodically discussed and tracked as formal agenda items at the monthly MSC meetings.

7.2 Risk Reporting & Escalation

Projects will report risks to SID on a monthly basis (or as needed). Projects will also report risks to their oversight representative(s) using Appendix E: Risk Management Form of the DOF IT Project Oversight Framework reporting guidelines, and any other reporting guidelines of the oversight entity.

Projects will define risk escalation as a function of Project Criticality (see DOF's IT Project Oversight Framework, Section 2) and Risk Severity (see above) as a means for determining which risks will be escalated from department to Agency and from Agency to Finance. Not all risks require escalation, and escalation of project risks will not necessarily result in a change in project criticality.

Note: Projects are free to create a project-specific matrix and are not required to adhere to the SAMPLE shown below. Projects are to define "how" risks are escalated and through what chain of command they are submitted (until they reach their eventual reporting destination).



		Risk Severity		
		High	Medium	Low
Project Criticality	High	DOF	CHHS	CDSS / HHSDC / SID
	Medium	CHHS	CHHS	CDSS / HHSDC / SID
	Low	CHHS	CDSS / HHSDC / SID	

7.3 Control

Projects may include a Level of Control category with the four choices as shown below. It will be important that an integrated risk management system be able to distinguish the level by which risks need to be addressed (e.g., SID-Level, HHSDC Director-Level, PM-Level, etc.). This category could be specifically used to indicate who has the authority to influence the risk.

Level of Control	**Definition**
No Control	No resource within SID or HHSDC can control the outcome of this risk
Minimal	The SID Assistant Director or HHSDC Director has the authority to control the outcome of this risk
Moderate	The Project Manager has the authority to control the outcome of this risk
High	A Project Team Leader has the authority to control the outcome of this risk

8 COMMUNICATION OF RISKS

Projects will ensure ongoing communication that enables the sharing and effective management of risks throughout the project life cycle. Projects will include communication of project risks as an ongoing activity that is part of each of the steps mentioned above and documented in the project Risk Management Plan.

8.1 Lessons Learned Repository on Risk

Projects are encouraged to include a review of historical findings of prior projects (as taken from the PRD) and use these findings during the acquisition planning process or start of new life cycle phase. Confidentiality of items in the risk database will need to be taken into account before releasing risk information across projects.

8.2 Public Domain Nature of Risk

Some projects have “confidential” risks that could have legal ramifications if inadvertently released. The notion of “public” risks needs to be considered when deciding to offer risks for the purpose of lessons learned. Projects are to coordinate release of potentially sensitive information with their legal advisors before submitting items to the public.

APPENDIX A- SEI Risk Taxonomy Categories

A. PRODUCT ENGINEERING	B. DEVELOPMENT ENVIRONMENT	C. PROGRAM CONSTRAINTS
1. REQUIREMENTS	**1. DEVELOPMENT PROCESS**	**1. RESOURCES**
a. Stability	a. Formality	a. Schedule
b. Completeness	b. Suitability	b. Staff
c. Clarity	c. Process Control	c. Budget
d. Validity	d. Familiarity	d. Facilities
e. Feasibility	e. Product Control	**2. CONTRACT**
f. Precedent	**2. DEVELOPMENT SYSTEM**	a. Type of Contract
g. Scale	a. Capacity	b. Restrictions
2. DESIGN	b. Suitability	c. Dependencies
a. Functionality	c. Usability	**3. PROGRAM INTERFACES**
b. Difficulty	d. Familiarity	a. Customer
c. Interfaces	e. Reliability	b. Associate Contractors
d. Performance	f. System Support	c. Subcontractors
e. Testability	g. Deliverability	d. Prime Contractor
f. Hardware Constraints	**3. MANAGEMENT PROCESS**	e. Corporate Management
g. Non-Developmental Software	a. Planning	f. Vendors
3. CODE AND UNIT TEST	b. Project Organization	g. Politics
a. Feasibility	c. Management Experience	
b. Testing	d. Program Interfaces	
c. Coding/Implementation	**4. MANAGEMENT METHODS**	
4. INTEGRATION AND TEST	a. Monitoring	
a. Environment	b. Personnel Management	
b. Product	c. Quality Assurance	
c. System	d. Configuration Management	
5. ENGINEERING SPECIALTIES	**5. WORK ENVIRONMENT**	
a. Maintainability	a. Quality Attitude	
b. Reliability	b. Cooperation	
c. Safety	c. Communication	
d. Security	d. Morale	
e. Human Factors		
f. Specifications		